IN THE UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH CAROLINA
CHARLESTON DIVISION

IN THE MATTER OF THE SEARCH OF **(1) Black Apple iPhone in black leather case** **(2) Black Apple iPhone, cracked on front and back with no case** **(3) Black TCL cell phone with no case** **(4) Silver Apple iPad S/N DMPPTQ0GFK11** **(5) HP Compaq Pro 6300 tower computer S/N 2UA3421DTJ** **(6) Silver HP laptop computer S/N 5CG136CHD1** **(7) Toshiba disk drive S/N 12SJC01YT** **(8) Two (2) 32GB SD cards** **(9) Sandisk 64GB thumb drive**	Case No. 2:23-cr-00787

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Robert Callahan, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property – digital devices – which are currently in law enforcement possession as described in Attachment A, and the extraction from that property of electronically stored information as described in Attachment B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), and have been so employed since 2009. I have a Bachelor of Science degree in Criminal Justice received from the University of South Carolina. I am a graduate of the Federal

Law Enforcement Training Center and the ATF National Academy. I am currently assigned to the ATF Charleston Field Office within the Charlotte Field Division. I have participated in numerous investigations involving state and federal firearm violations to include: the illegal possession of firearms, firearms trafficking, straw purchasing of firearms, dealing in firearms without a license, and firearms classified under the National Firearms Act (NFA), among others. I have also participated in numerous investigations involving state and federal narcotics violations. Accordingly, I am thoroughly familiar with the investigative techniques used in these investigations, such as the use of undercover agents, the use of cooperating witnesses and confidential informants, surveillance, search and seizure warrants, and the extraction and analysis of data from digital devices. As a federal agent, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. § 922(o) (knowing possession of machinegun), 26 U.S.C. § 5861(d) (possession of unregistered firearm), 26 U.S.C. § 5861(e) (transfer of firearm in violation of chapter), 18 U.S.C. § 545(a) (smuggling goods into the United States), 26 U.S.C. § 5844 (importation of firearms into the United States), 26 U.S.C. § 5861(k) (Receipt or possession of unlawfully imported firearm), 18 U.S.C. § 922(g)(3) (Possession of a firearm by an unlawful user of a controlled substance), and 18 U.S.C. § 922(a)(6)

(Making of false statements in connection with the acquisition of a firearm) have been committed by Herman Tobiah WRIGHT ("WRIGHT"), a/k/a "Wink". There is also probable cause to search the Devices further described below and in Attachment A, for the things described in Attachment B, in accordance with Attachment C.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

5. The property to be searched is further described as:

- Black Apple iPhone in black leather case
- Black Apple iPhone, cracked on front and back with no case
- Black TCL cell phone with no case
- Silver Apple iPad S/N DMPPTQ0GFK11
- HP Compaq Pro 6300 tower computer S/N 2UA3421DTJ
- Silver HP laptop computer S/N 5CG136CHD1
- Toshiba disk drive S/N 12SJC01YT
- Two (2) 32GB SD cards
- Sandisk 64GB thumb drive

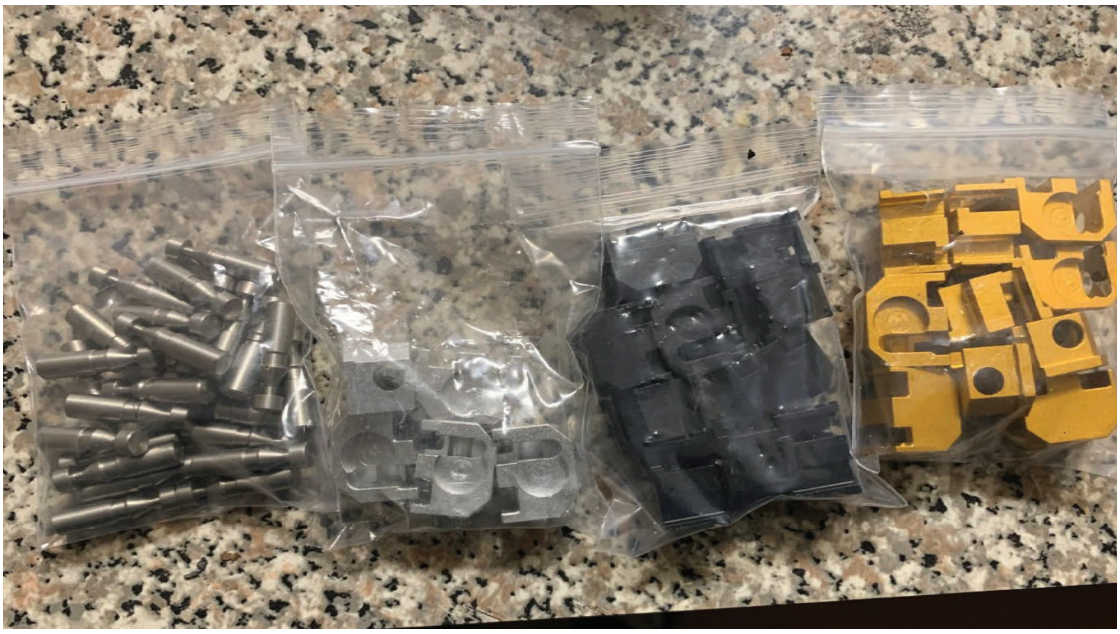
6. "The Devices" are currently located in the ATF Charleston Field Office, 1 Poston Rd, Suite 325, Charleston, SC 29407.

PROBABLE CAUSE

7. In December 2022, I reviewed the downloaded contents of a cell phone that had been seized from Carl Shedrick Hopkins pursuant to a federal search warrant. While reviewing the contents of the device, messages were discovered between Hopkins and an individual believed to be WRIGHT, a/k/a "Wink" discussing the acquisition and disposition of "switches" which I know, based on training and experience to be Glock conversion devices.

8. I reviewed several messages between Hopkins and phone number (404) 449-5544, labeled in Hopkins' phone as "Wink." I queried various law enforcement databases, and the aforementioned phone number is associated with WRIGHT. In response to a Court Order for records associated with the aforementioned phone number, T-Mobile records indicate the account billing address as, Herman Wright, PO Box 15955, Lenexa KS 66285.

9. On January 12, 2022, "Wink" sent the following message to Hopkins, "im the real life Ghost no tv show but I got switches on deck for the glocks how many were you need." Hopkins replied, "I need couple to get rid I got sum plays for em yes sir!!!" "Wink" then sent Hopkins the following photograph of suspected Glock conversion devices:



10. After sending the photograph of the suspected Glock conversion devices, "Wink" sent a message that stated, "Delete that pic asap tho."

11. Hopkins sent "Wink" a photograph of an AR-style firearm and "Wink" stated, "I got the full switches for them too lol" and Hopkins replied, "Yep need it ASAP" and "Boy I get rid of all em in one day."

12. "Wink" then sent Hopkins a message that stated, "I want 300 I'll do 150 for you so can cushion I'll bring you some when I come home that's what im trying set up…Plays for em."

13. On January 29, 2022, "Wink" sent the following message to Hopkins, "Did that pack I give you have extra little pieces in it."

14. On July 3, 2022, a message from the Facebook messenger account, "Tobiah Wright" to Hopkins stated, "I'm coming this week was waiting on the rest of the switches."

15. I am familiar with machinegun conversion devices and have been involved in prior investigations involving Glock and AR-type conversion devices. I know that often, due to their classification as machineguns and being regulated by ATF, these devices are commonly ordered online from another country and mislabeled with deceptive descriptions to conceal the true contents of the package, in an effort to divert the attention of law enforcement.

16. I requested inbound international shipments from Homeland Security Investigations (HSI) for parcels sent to WRIGHT. The shipment information indicated that "Tobiah Wright" has received approximately thirty (30) shipments.

17. The data showed approximately five (5) shipments between November 2022 and June 2023, from China, addressed to "Tobiah Wright" at 255 E 9th North St Apt 24C, Summerville, SC. I queried the South Carolina Department of Motor Vehicles and discovered that WRIGHT's listed address is the same as above.

18. The data showed approximately seventeen (17) shipments between February 2022 and January 2023, addressed to "Tobiah Wright" at 2194 Briarcliff Rd NE, Atlanta, GA. Some of the shipments included "Apt 7" in the address. I queried various law enforcement databases and reviewed law enforcement reports, and the aforementioned address is associated with WRIGHT.

19. The data showed approximately eight (8) shipments between August 2015 and January 2022 addressed to "Tobiah Wright" at other addresses.

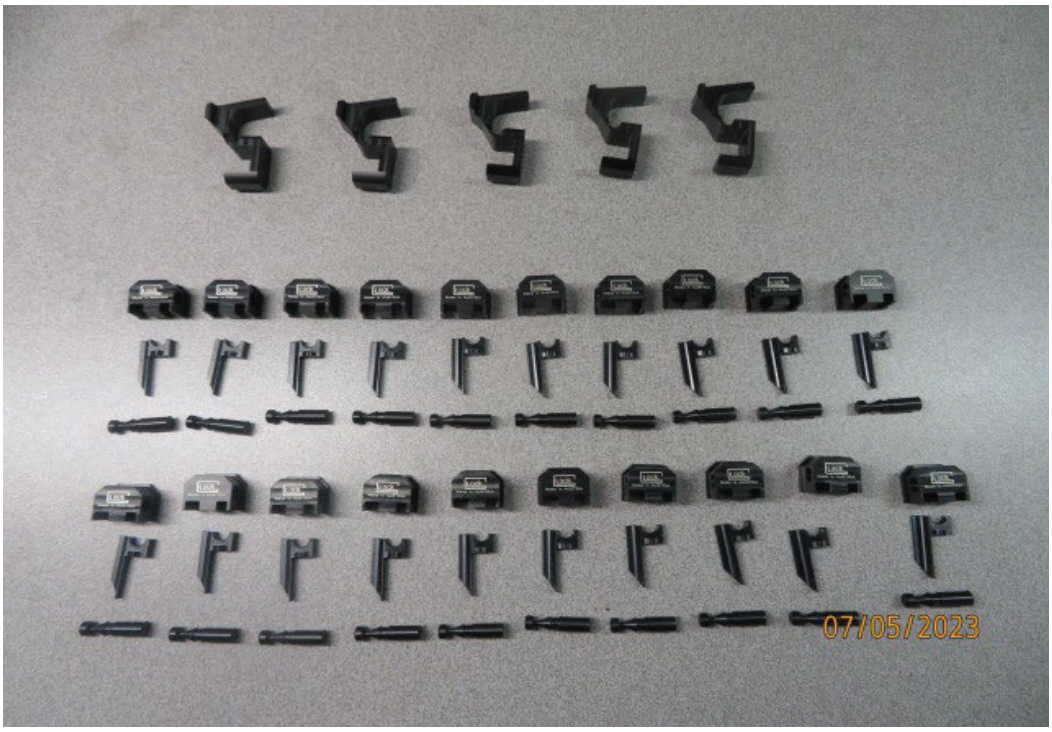
20. The descriptions of some of the items shipped included, "valve", "suspension component", "clip", "aluminum part", "pneumatic tool small safety valve" and "wind chimes" among others.

21. I queried the South Carolina Department of Motor Vehicles for vehicles registered to WRIGHT and discovered among others, a 2001 Ford F150 pickup truck bearing SC license plate VAU333 and a 2012 Ford Mustang, bearing SC license plate WRI535.

22. On December 15, 2022, I conducted surveillance and observed WRIGHT's Ford F150 parked directly in front of 255 E 9th North St, Apt 24C, Summerville, SC 29483.

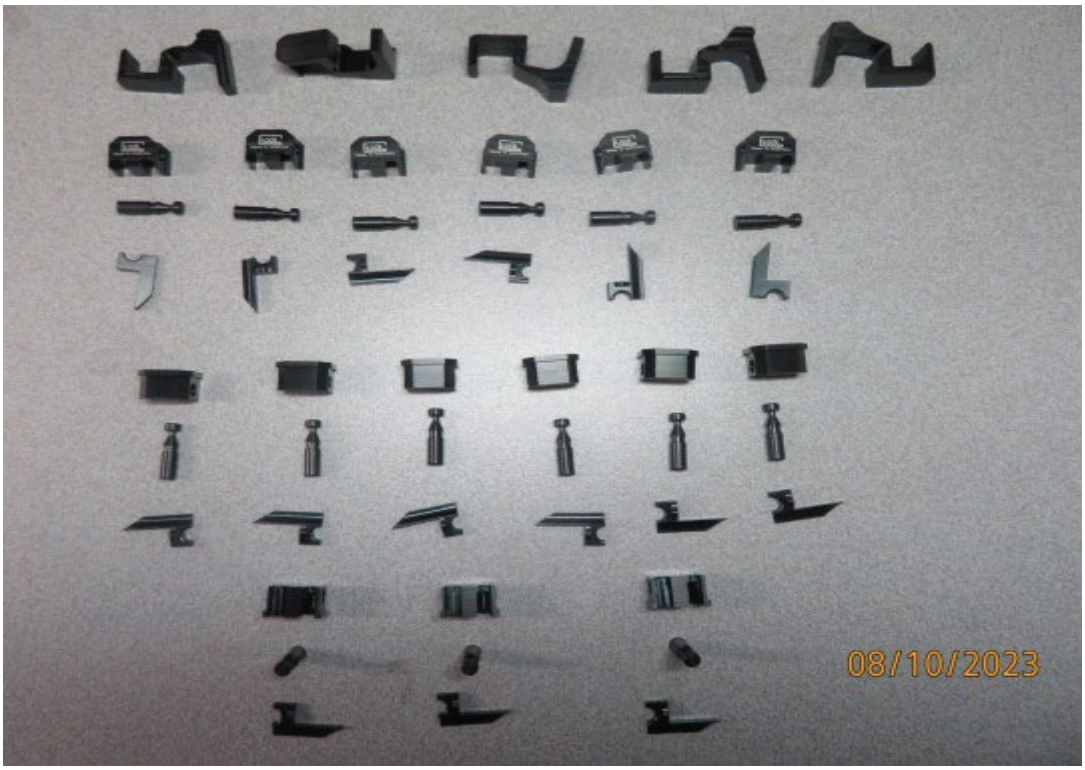
23. On December 21, 2022, ATF SA James Dougherty conducted surveillance and observed WRIGHT's Ford F150 parked in the parking lot across from 2194 Briarcliff Rd NE, Apt 7, Atlanta, GA 30329.

24. On July 5, 2023, I was notified by HSI that Customs and Border Protection (CBP) intercepted a parcel addressed to consignee "Tobiah Wright" at 255 E 9th North St, 24C, Summerville, SC with associated phone number (404) 449-5544. The package originated from China and arrived at JFK Airport on or about April 11, 2023, and subsequently placed on hold by CBP on or about April 12, 2023. I was advised that the package was searched by CBP on July 5, 2023, and twenty (20) Glock conversion devices and five (5) AR-type conversion devices were contained in the package, as identified by the photograph below.



25. On July 13, 2023, I received a verbal classification from FATD that all of the submitted devices are in fact, machineguns. The verbal classification was followed up with a Report of Technical Examination received from FATD on July 27, 2023.

26. On August 7, 2023, I was notified by HSI that Customs and Border Protection (CBP) intercepted a parcel addressed to consignee "Tobiah Wright" at 255 E 9th North St, 24C, Summerville, SC 29483 with associated phone number (404) 449-5544. The package originated from China and arrived at JFK Airport on or about August 6, 2023, and subsequently placed on hold by CBP. I was advised that the package was searched by CBP on August 10, 2023, and fifteen (15) Glock conversion devices and five (5) AR-type conversion devices were contained in the package, as identified by the photograph below.



27. On August 31, 2023, I received a Report of Technical Examination from FATD that all of the devices from the second seized package are in fact, machineguns.

28. On August 24, 2023, a federal search warrant was executed at WRIGHT's residence in Summerville, SC. During the search warrant, investigators seized seven (7) firearms, to include a shotgun that appeared to have been modified with the stock and barrel shortened, thus making it a firearm requiring proper registration under the National Firearms Act (NFA). Investigators seized four (4) suspected Glock switch bodies from within the residence and another suspected Glock switch body and selector switch from a vehicle associated with WRIGHT. Investigators seized suspected marijuana and a substance that field tested positive for fentanyl. Investigators also seized the aforementioned electronic Devices from the residence.

29. While the search warrant was being executed, I advised WRIGHT that he was not under arrest but that he was being detained. I read WRIGHT his *Miranda* warning, and WRIGHT indicated that he understood his rights and wished to speak with me. During the interview,

WRIGHT admitted to being an unlawful user of marijuana and that he has been using marijuana daily since he was in high school. WRIGHT stated he was aware that there was marijuana inside the residence and that he was smoking the marijuana. WRIGHT indicated that he ordered a lot of products and supplements from China to include the bag containing a white powder that field tested positive for fentanyl that was seized from the residence.

30. WRIGHT stated he knows what Glock switches are and stated that the penalty is ten (10) years in prison if you get caught with a Glock switch. I asked WRIGHT about packages containing Glock switches being shipped to his address, in his name. WRIGHT stated that he knew how to get the Glock switches from China, and he would send people the link to order them and would allow them to have the Glock switches shipped to his address. WRIGHT indicated that because he is ex-military, the packages ordered from China would draw less attention from law enforcement if they were being shipped to him as the consignee because most of the people that were ordering the Glock switches had bad records and couldn't afford to get in trouble.

31. WRIGHT indicated that he played the "middleman" and that if a large order of Glock switches was shipped to his residence, he would help people sell the Glock switches by contacting potential buyers to set up sales. WRIGHT stated he sent the link to purchase the Glock switches to a lot of people but that he never ordered/paid for any Glock switches. WRIGHT stated the websites they used to purchase the Glock switches were, www.dhgate.com, www.alibaba.com, or www.aliexpress.com. WRIGHT indicated that his order history from China could be reviewed via his account on the "Alibaba" website. WRIGHT stated the Glock switches cost $8.00 a piece online and they could resell them for $250 to $300 a piece on the street. WRIGHT stated the AR-type conversion devices would sell for as much as $400.00 to $450.00 a piece on the street. WRIGHT stated that the individuals that ordered the Glock switches would sometimes contact him

and ask if a package had arrived at his residence. In relation to the aforementioned messages exchanged with Hopkins, WRIGHT stated he did provide Hopkins with five (5) Glock switches.

32. WRIGHT stated that the firearms seized from his residence are his but that his girlfriend, Brianna Gaddy purchased the firearms for him. WRIGHT further explained that he would order the firearms online and have them shipped to a federal firearms licensee (FFL) in Georgia where he and Gaddy were residing at the time. WRIGHT stated that because he did not have a Georgia identification card, Gaddy would pose as the purchaser of the firearms and complete the ATF Form 4473, Firearm Transaction Record at the FFL. WRIGHT stated that he paid for the firearms with his money. WRIGHT stated he also has bill of sale forms, indicating that Gaddy transferred the firearms to WRIGHT. WRIGHT indicated that he could print the bill of sale forms from his computer.

33. The firearms recovered from the search warrant were entered into the e-Trace system. As of the time of this affidavit preparation, two (2) e-Trace queries of the firearms recovered from the residence that WRIGHT indicated were his, have been completed. The queries indicated that both firearms were purchased by Gaddy from FFLs in Georgia.

34. WRIGHT was queried in the ATF Federal Licensing System to determine if WRIGHT possesses any type of federal firearms license, and I was advised WRIGHT does not possess any licenses in the Federal Licensing System.

35. The ATF National Firearms Act Division is the only federal authority permitted to regulate firearms covered by the National Firearms Act (NFA). The National Firearms Act Division processes all applications to make, export, transport and register NFA firearms and destructive devices. The Industry Processing Branch (IPB) processes all non-government application to make, export, transfer and register NFA firearms. The IPB also maintains the

National Firearm Registration and Transfer Record (NFRTR), the central registry for all items regulated under the NFA.

36. WRIGHT was queried in the NFRTR, and it was determined that WRIGHT does not have any firearms falling under the purview of the NFA registered with ATF.

37. I am aware through training and experience and conferring with other Special Agents, to include ATF Interstate Nexus Experts, that the firearms (non NFA) seized from WRIGHT by law enforcement did affect interstate commerce.

38. I know that cell phones, computers and other digital devices are often used by certain individuals to facilitate the commission of criminal acts. I know that certain individuals will often utilize multiple digital devices, acquire new devices, or discard devices to avoid detection. Further, I am aware that incriminating evidence is often located within text messages, as well as photos and videos contained on cell phones and within web activity and saved documents on computers, hard drives, and other internal and external storage devices. Additionally, call logs (for incoming, outgoing, and missed calls), stored contact lists, and location information have proven to be valuable evidence in criminal cases. I know that individuals prohibited from possessing firearms or those individuals that want to conceal ownership of firearms, often utilize a straw purchaser to purchase firearms on their behalf from an FFL and that on occasion, the prohibited person will accompany the straw purchaser to the FFL. The revelation of these locations is valuable to an investigation and can aid in identifying possible co-conspirators. Moreover, I am familiar with technology, such as Cellebrite mobile data transfer equipment, that allows law enforcement investigators to harvest data (such as incoming and outgoing text messages, photos, videos, call logs, and contacts) from cell phones. In addition, based on my experience, I know that individuals engaged in the illegal acquisition, possession, and dissemination of firearms often

utilize mobile telephones and other digital devices to communicate with customers, receive orders, make purchases, create ledgers and bill of sale forms, and to arrange for dissemination of the firearms. Often times, photographs are taken of the firearms to facilitate the transaction or to post the photographs in online firearm classified advertisements. These photographs can be maintained on mobile telephones, computers and other digital devices. I also know that digital devices reveal evidence of user attribution, showing who used or owned the device at the time it was seized by law enforcement.

39. The Devices are currently in the lawful possession of ATF and stored at the ATF Charleston Field Office, 1 Poston Rd, Suite 325, Charleston, SC 29407. The Devices came into the ATF's possession during the execution of a federal search warrant at WRIGHT's residence. Therefore, while ATF might already have all necessary authority to examine the Devices, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Devices will comply with the Fourth Amendment and other applicable laws.

40. In my training and experience, I know that the Devices have been stored in a manner in which the contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of ATF.

TECHNICAL TERMS

41. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. "Digital device," as used herein, includes the following three terms and their respective definitions:

1) A "computer" means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

2) "Digital storage media," as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks ("DVDs"), USB flash drives, flash memory cards, and internal and external hard drives.

3) "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

b. "Wireless telephone" (or mobile telephone, or cellular telephone), a type of digital

device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through "wi-fi" networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional "land line" telephones, computers, and other digital devices. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system ("GPS") locating and tracking technology, and accessing and downloading information from the Internet.

c. A "tablet" is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, "wi-fi" networks, or otherwise. Tablets typically contain programs called applications ("apps"), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

d. A "GPS" navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated "GPS") to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or

walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. Internet Protocol ("IP") Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

f. The "Internet" is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

g. "Internet Service Providers," or "ISPs," are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet,

including via telephone-based dial-up and broadband access via digital subscriber line ("DSL"), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

h. "Domain Name" means the common, easy-to-remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first-level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second-level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

i. "Cache" means the text, image, and graphic files sent to and temporarily stored by a user's computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website in the future.

42. Based on my training, experience, and research, I know that certain cell phones and tablets have capabilities that allow them to serve as a wireless telephone, digital camera, portable

media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, and sometimes by implication who did not, as well as evidence relating to the commission of the offenses under investigation.

COMPUTERS, ELECTRONIC/MAGNETIC STORAGE AND FORENSIC ANALYSIS

43. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found within the Devices, in whatever form they are found. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that there is probable cause to believe that the records and information described in Attachment B will be stored in the Devices for at least the following reasons:

a. Individuals who engage in criminal activity, including the illegal importation, possession and dissemination of machinegun conversion devices use digital devices, like the Devices, to access websites to facilitate illegal activity and to communicate with co-conspirators; to store on digital devices, like the Devices, documents and records relating to their illegal activity, which can include order history, online communication, email, text or other "Short Message Service ("SMS") messages, and photos; contact information of co-conspirators, including telephone numbers, email addresses and identifiers for social media accounts.

b. Individuals who engage in the foregoing criminal activity, in the event that they

change digital devices, will often "back up" or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

44. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes

described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital device(s) were used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the Device(s) at issue here because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device(s), not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and

other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

f. I know that when an individual uses a digital device to unlawfully import, possess, and sell machinegun conversion devices, the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense and the identities of those perpetrating it.

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

45. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of

information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. Recovery of "residue" of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a

number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting "keyword" search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format ("PDF"), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of

data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as "AES-256 encryption" to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

46. In searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

a. The digital devices, and/or any digital images thereof created by law enforcement, sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

b. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by "opening," reviewing, or reading the images or first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "keyword" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

c. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the Device(s) will be specifically chosen to identify the specific items to be seized under this warrant.

AUTHORIZATION TO SEARCH AT ANY TIME OF THE DAY OR NIGHT

47. Because forensic examiners will be conducting their search of the digital devices in a law enforcement setting over a potentially prolonged period of time, I respectfully submit that good cause has been shown, and therefore request authority, to conduct the search at any time of the day or night.

CONCLUSION

48. I submit that this affidavit supports probable cause for a warrant to search the Devices described in Attachment A and to seize the items described in Attachment B, in accordance with Attachment C.

This affidavit has been reviewed by SAUSA Carra Henderson.

Respectfully submitted,

ROBERT CALLAHAN Digitally signed by ROBERT CALLAHAN Date: 2023.09.05 13:30:29 -04'00'

Robert Callahan
Special Agent
Bureau of Alcohol, Tobacco, Firearms & Explosives

Subscribed and sworn to before me
on September 6, 2023

HON. MOLLY H. CHERRY
UNITED STATES MAGISTRATE JUDGE